PRIVACY POLICY

Last Updated: 02nd December, 2025

This Privacy Policy describes how the **Secure Data Sharing Platform for Controlled Access** (“Platform”, “we”, “our”, “system”) collects, uses, stores, protects, and manages user information. The Platform is designed with centralized gateway monitoring, role-based access control, immutable logging, and AI-assisted anomaly detection to ensure secure and compliant data-sharing operations.

By accessing or using the Platform, users agree to the practices outlined in this Policy.

1. Purpose of Data Collection

The Platform collects and processes data exclusively to:

- Authenticate users and enforce role-based access control;
- Monitor and regulate data interactions passing through the centralized gateway;
- Generate tamper-proof audit logs for accountability and compliance;
- Detect and respond to suspicious activities using AI-based anomaly detection;
- Maintain the security, integrity, and operational continuity of the system.

2. Information We Collect

2.1 User-Provided Information

We collect information directly entered by users during registration, login, and system usage, including:

- Name or user identifier;
- Login credentials;
- Assigned user role (Owner, Supervisor, Manager, Employee);

2.2 Automatically Collected Information

Through the secure gateway, the system automatically records:

- Device identifiers (IP address, MAC address);
- Login attempts and authentication status;
- Timestamped access logs;
- Network traffic metadata;
- Actions performed within user privilege limits;
- Blocked or unauthorized access attempts.

3. How We Use Your Information

Collected information is used for the following purposes:

- **Authentication & Authorization:** Verifying user identity and applying predefined RBAC policies.
- **Secure Data Flow:** Controlling and approving user access based on stored privileges.
- **Monitoring & Logging:** Creating complete, immutable logs of all interactions within the system.
- **Threat Detection:** Identifying irregular or unauthorized activity using AI-based models.
- **Compliance & Forensics:** Supporting audits, investigations, and organizational reporting.

Your data is **not** used for marketing, advertising, or non-security-related activities.

4. Data Security Measures

4.1 Gateway-Level Enforcement

All data traffic is routed through a centralized hardware security gateway, ensuring consistent monitoring, validation, and control.

4.2 Encryption

Secure communication channels and encrypted storage mechanisms (such as AES/RSA) are used to protect sensitive information during transmission and storage.

4.3 Immutable Logging

Audit logs are stored using append-only or blockchain-inspired methods to ensure they cannot be altered, deleted, or manipulated by any user, including administrators.

5. Data Sharing & Disclosure

We do **not** sell, rent, or disclose user data to third parties.

Information may be shared only when required to:

- Comply with legal or regulatory obligations;
- Support internal audits or investigative procedures;
- Maintain or restore the security and functionality of the Platform.

All access to data is strictly governed by predefined privileges and internal security policies.

6. User Rights

Users may, subject to role permissions and system policies:

- View their own activity logs;

- Request updates to their profile information;
- Request account deactivation or removal (where applicable).

Note: Immutable audit logs cannot be modified or deleted under any circumstances, as they serve as permanent security records.

7. Data Retention

- User accounts and related information are retained for the duration of system use or until deactivated by an authorized administrator.
- Audit logs and security records are retained indefinitely or as defined by organizational policy.
- Immutable logs cannot be removed or overwritten.

8. Use of Cookies and Local Storage

If the Platform’s web dashboard is accessed, cookies or local storage may be used to maintain secure session tokens. These are used strictly for authentication and session management, not for tracking or advertising.

9. Updates to This Policy

We may revise this Privacy Policy periodically. Updates will be communicated through the Platform, and continued use constitutes acceptance of the revised policy.

10. Contact Information

For questions, concerns, or requests related to this Privacy Policy, please contact:

Email: superadmin@secureshare.com
Address: Bengaluru